

JSP 602 Instruction	1001	Applicability	Applications, Data/Information, Integration, Network/Communications, Security
Configuration Identity	Version: 01.02 Amended: 2009-03-02 Reviewed: 2006-06-15	Epoch Applicability	2005 - 2009

JSP 602: 1001 - Application Architecture

Outline

Description: This policy leaflet provides high-level direction on the architecture of applications that MOD hosts on its systems and infrastructure. An Application Architecture defines the application components and their relationships. The components of an Application Architecture are hardware, software, data, security, processes and communications infrastructure. Each component will have defined standards and products. The relationships include integration, interface and security aspects.

Reasons for Implementation: Adoption by MOD of an Application Architecture will assist in reducing through-life costs of applications. It will also assist in enhancing internal consistency of applications, and interoperability between applications and their supporting infrastructure.

Applications used by MOD, whether developed in-house or bought-in, must be standardised to maximise business benefit by making effective and efficient use of applications and development staff. Compliance with this policy will facilitate the delivery of coherent applications that meet business and operational needs.

Issues: Many of the applications MOD procures are COTS and this inevitably limits MOD's influence on the application architecture. However, the policy defined in this leaflet largely reflects commercial best practice and should be used as one of the benchmarks for assessing applications.

Guidance: In battlespace environments, the default option should be to access applications through a browser interface and host the majority of application functionality on server devices. However, where it can be demonstrated that conforming to this principle would significantly degrade other required system properties, such as performance and reliability, other architectural options are permitted. Such options will only be accepted where there is sufficient and valid justification.

Off-the-shelf software components, either commercial or Open Source should be used in preference to bespoke development. The interchange standards that should be used for information exchange between applications are covered in more detail in JSP 602 1017: Middleware and Web Services.

This leaflet is outside the scope of both the e-GIF and the NC3TA.

Policy

Strategic

1001.01: Web Services

1001.01.01 Applications hosted on the Global Information Infrastructure shall utilise Web Services technologies and be accessed through a non-proprietary browser interface.

1001.01.01.01 Where a client-server model of application segmentation is being used, and there is sufficient and reliable communications and network capacity, applications functionality shall be hosted on server devices.

Significant proportion of processing and data storage shall not be hosted on locally situated devices (see comment).

Comment: Application developers must consult infrastructure providers to determine if there is adequate and reliable communications and network capacity, sufficient to support the preferred method of application provision. Only in justifiable circumstances, for example when communications and networks have insufficient capacity, and/or they are unreliable should significant proportions of processing or storage be hosted locally on a client device or system. Infrastructure providers must also be consulted to ascertain the performance, functionality and capacity of client devices, in order to determine their compatibility with the chosen architectural option.

1001.02: Performance Requirements

1001.02.01 An application must perform within required limits, whether it is being run in the strategic domain (e.g. an office environment) or in a deployed or tactical domain. For these requirements to be met the following issues shall be addressed in the SRD:

1001.02.01.01 Logical and physical location of data and code (i.e. use of n-tier architecture);

1001.02.01.02 Use of common facilities provided by the host infrastructure, e.g. replication, caching, proxying and directory facilities;

1001.02.01.03 WAN connectivity requirements (see JSP602: 1030 - Wide Area Bandwidth);

1001.02.01.04 Configuration management (see JSP602: 1034 - Network Mapping and Configuration Management);

1001.02.01.05 Performance requirements;

1001.02.01.06 Size, location(s), mobility and variability of client base;

1001.02.01.07 Security (Confidentiality, Integrity, and Availability) and business continuity (including backup and recovery) (see JSP602: 1036 - Security Architecture);

1001.02.01.08 Business requirements.

Comment: WAN Bandwidth requirements are the subject of JSP 602 1030: Wide Area bandwidth; Configuration Management is the subject of JSP 602 1034: Network Mapping & Configuration Management; Security is the subject of JSP 602 1036: Security Architecture.

Strategic (continued)

<u>1001.03: Use of COTS products</u>

1001.03.01 COTS products, including both conventional commercial products and Open Source components, shall be favoured over bespoke solutions.

<i>Comment:</i> Projects and application developers shall, in first instance, seek to use suitable COTS products, rather than developing bespoke solutions. If bespoke development is required it should be implemented so that it is reusable by other applications in the future. In-house developed or customised software shall be accompanied by design documentation to support maintenance and future enhancement.

Deployed

As for Strategic domain.

Tactical

As for Strategic domain.

Remote

As for Strategic domain.

Responsibility for Implementing the Policy

Implementation of this policy shall be the responsibility of all IPTs (and their suppliers) that provide applications to MOD.

Procedure

Not Applicable.

Relevant Links

JSP602: 1017 - Middleware and Web Services

JSP602: 1030 - Wide Area Bandwidth

JSP602: 1034 - Network Mapping and Configuration Management

JSP602: 1036 - Security Architecture

A glossary of terms and abbreviations used within this document is available [here](#).

Instructions on how to read a JSP602 leaflet are available [here](#).

Compliance

Stage	Compliance Requirements
Initial Gate/DP1	MOD Projects shall submit a formal declaration that they have read and understood the policy and sought guidance from the SME(s).
Main Gate/DP2	MOD Projects shall present the sections of their SRD that cover the aspects defined in this policy. They shall also submit high-level architecture views/representations of the application (using MODAF views).
Release Authority/DP5	MOD Projects (supported by their equipment suppliers) shall provide evidence of their compliance policy by submitting detailed architecture views/representations of the application (using MODAF views).